IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

SECURUS TECHNOLOGIES, INC., Plaintiff, v. GLOBAL TEL*LINK CORPORATION, Defendant.	CIVIL ACTION NO. 3:13–CV–03009–K

PLAINTIFF/COUNTERCLAIM–DEFENDANT SECURUS TECHNOLOGIES, INC.'S RULE 12(C) MOTION FOR JUDGMENT ON THE PLEADINGS BASED ON INVALIDITY OF THE COUNTERCLAIM PATENTS UNDER 35 U.S.C. § 101 AND BRIEF IN SUPPORT

TABLE OF CONTENTS

I. INTRODUCTION 1

II. BACKGROUND OF THE ASSERTED PATENTS 3

A. The ’359 and ’171 patents both describe a general process for determining whether an inmate has had unauthorized communications. 3

B. The ’359 and ’171 patents describe and claim nothing more than comparing a first piece of information to a database of information. 6

III. LEGAL STANDARDS 7

A. Standard for motion for judgment on the pleadings under Rule 12(c). 7

B. Patent eligibility is appropriately resolved at the pleading stage. 8

C. The Court may consider the pleadings, documents attached to or referenced in the pleadings, and material subject to judicial notice. 9

D. Standard for patentable subject matter under 35 U.S.C. § 101. 10

IV. POINTS AND AUTHORITIES 12

A. The claims of the ’359 and ’171 patents are directed to the ineligible abstract idea of determining if an inmate has had unauthorized communications. 12

1. The ’359 patent claims fail the first step of the Mayo analysis. 13

2. The ’171 patent claims fail the first step of the Mayo analysis. 15

B. The additional elements — generic computers, databases, software, and storage, all performing conventional tasks — do not supply an inventive concept. 18

V. CONCLUSION 20

TABLE OF AUTHORITIES

CASES

Accenture Global Servs. GmbH v. Guidewire Software, Inc.,
728 F.3d 1336 (Fed. Cir. 2013) 9, 12, 18

Alice Corp. Pty. Ltd. v. CLS Bank International,
134 S. Ct. 2347 (2014) 11, 12, 15, 18

Bancorp Servs., L.L.C. v. Sun Life Assur. Co. of Can. (U.S.),
687 F.3d 1266 (Fed. Cir. 2012) 18, 21

Bell Atl. Corp. v. Twombly,
550 U.S. 544 (2007) 9

Bilski v. Kappos,
561 U.S. 593 (2010) 11, 15, 19

buySAFE, Inc. v. Google, Inc.,
765 F.3d 1350 (Fed. Cir. 2014) 12, 18

Collins v. Morgan Stanley Dean Witter,
224 F.3d 496 (5th Cir. 2000) 10

Content Extraction & Transmission, LLC v. Wells Fargo Bank Nat'l Ass'n,
776 F.3d 1343 (Fed. Cir. 2014) 9, 11

CyberSource Corp. v. Retail Decisions, Inc.,
654 F.3d 1366 (Fed. Cir. 2011) 21

DDR Holdings, LLC v. Hotels.com, L.P.,
No. 2013–1505, 2014 U.S. App. LEXIS 22902, 2014 WL 6845152 (Fed. Cir. 2014) 2

Dealertrack, Inc. v. Huber,
674 F.3d 1315 (Fed. Cir. 2012) 9

Genetic Techs. Ltd. v. Bristol-Myers Squibb Co.,
No. 12–394–LPS, 2014 WL 5507637 (D. Del. Oct. 30, 2014) 9, 10

Gorski v. The Gymboree Corp.,
No. 14–CV–01314–LHK, 2014 WL 3533324 (N.D. Cal. July 16, 2014) 9

Hockerson-Halberstadt, Inc. v. Avia Group Int'l, Inc.,
222 F.3d 951 (Fed. Cir. 2000) 10

Iconfind, Inc. v. Google, Inc.,
No. 2:11–CV–0319–GEB–JFM, 2012 WL 158366 (E.D. Cal. Jan. 18, 2012) 10

Jericho Systems Corp. v. Axiomatics, Inc.,
No. 3:14–CV–2281–K, 2015 WL 2165931 (N.D. Tex. May 7, 2015) 2, 3, 8, 9, 11

Johnson v. Johnson,
385 F.3d 503 (5th Cir. 2004) 8

Loyalty Conversion Sys. Corp. v. Am. Airlines,
No. 2:13–CV–655, 2014 WL 4364848 (E.D. Tex. Sept. 3, 2014) 8, 12, 21

Mayo Collaborative Services v. Prometheus Laboratories, Inc.
132 S. Ct. at 1297–98 ..... 10-13, 15, 16, 18

Morlock, L.L.C. v. JP Morgan Chase Bank, N.A.,
587 F. App'x 86 (5th Cir. 2014) 10

OIP Techs., Inc. v. Amazon.com, Inc.,
788 F.3d 1359 (Fed. Cir. 2015) 9, 12, 20

STATUTORY AUTHORITIES

35 U.S.C. § 101 ..... 1, 3, 8-12, 17, 18, 21

RULES AND REGULATIONS

Fed. R. Civ. P. 12(c) 3, 8

Fed. R. Evid. 201 10

Plaintiff/Counterclaim-Defendant Securus Technologies, Inc. ("Securus") moves for judgment on the pleadings on Defendant/Counterclaim-Plaintiff Global Tel*Link's ("GTL") remaining patent-infringement counterclaims (Counts II and II) for U.S. Patent Nos. 7,085,359 ("the '359 patent") and 7,039,171 ("the '171 patent").[1]

I. INTRODUCTION

Because GTL's patents fail to meet the requirements for patent eligibility under 35 U.S.C. § 101, this Court should grant judgment on the pleadings in favor of Securus. The two patents GTL asserts in this action do nothing more than claim the abstract idea of determining if an inmate has had unauthorized communications. Recent Supreme Court cases have made clear, however, that patents directed to abstract ideas do not meet the threshold requirement for patent eligibility under section 101 and that simply invoking generic computers and computer components to implement the abstract idea, as in the '359 and '171 patents, will not make otherwise ineligible claims patent-eligible.

As the Court is aware, when a criminal or suspected criminal is incarcerated, the inmate forfeits some of the freedoms that persons outside the criminal-justice system enjoy. While some restrictions are obvious, others are less apparent but nevertheless important. For example, inmates are not free to communicate with or contact anyone that they desire, and the correctional institution must be able to detect unauthorized communications to prevent them from recurring. In particular, inmates are not permitted to communicate with the victims of their crimes, certain

[1] The '359 patent is included in the Appendix to this Motion, as Exhibit A, and the '171 patent is Exhibit B. While GTL's counterclaim asserts infringement of a third patent, No. 7,742,581 (Count IV), GTLs' counsel has advised that GTL will not pursue its claims of infringement of on the '581 and a true and correct copy of Global Tel*Link's Amended Disclosure of Asserted Claims and Preliminary Infringement Contentions showing the dropping of allegations for the '581 patent is included in the Appendix as Exhibit C.

witnesses, court personnel, co-conspirators, or accomplices. They are also not permitted to communicate with members of threat groups such as gangs or terrorist organizations. Likewise, inmates are prohibited from having unauthorized communications with employees of the correctional institution, as these communications are indicative of fraternization between inmates and the employees, something that is absolutely forbidden.[2]

The patents-in-suit describe a method of determining if an inmate has had unauthorized communications by simply comparing a first piece of information about a communication (such as a telephone number) to information stored in a database (such as a listing of phone numbers for threat-group members or facility employees) to identify matches. The claimed methods can be performed mentally, with paper records, or with generic computer elements like "storage," "processor," or "database." The patents explain that the alleged inventions can be implemented on a single "general purpose computer," can be implemented in software or in hardware or both, and are not tied to any particular technology.

Under established law, this type of abstract idea is not eligible for patent protection, even where there are some references to computerized implementations. As this Court recently held, "the recitation of generic computer limitations does not make an otherwise ineligible claim patent eligible." *Jericho Systems Corp. v. Axiomatics, Inc.*, No. 3:14–CV–2281–K, 2015 WL 2165931, at *7 (N.D. Tex. May 7, 2015) (citing *DDR Holdings, LLC v. Hotels.com, L.P.*, No. 2013–1505, 2014 U.S. App. LEXIS 22902, 2014 WL 6845152 (Fed. Cir. 2014)).The claims here

[2] The historic problem of inmate-employee fraternization was recently brought to the forefront of public attention when two prison employees at New York's Clinton Correctional Facility were accused of aiding in the escape of two inmates. *See* N. Remnick, *Escapees' Fraternizing with Prison Workers Doesn't Surprise Experts*, N.Y. Times, June 30, 2015, *available at* http://www.nytimes.com/2015/07/01/nyregion/escapees-fraternizing-with-prison-workers-doesnt-surprise-experts.html?_r=0

are even more abstract than those found patent ineligible in *Jericho Systems*. Because the two patents at issue in this action are invalid under 35 U.S.C. § 101, the Court should grant judgment in favor of Securus under Rule 12(c) of the Federal Rules of Civil Procedure.

II. BACKGROUND OF THE ASSERTED PATENTS

The two asserted patents are related to each other, as the ’171 patent issued from an application that was a continuation-in-part of the ’359 patent. Compare Appendix, Ex. A, cover (Application No. 10/325,839) [App. 2] with Ex. B, cover (stating that ’171 patent is “continuation-in-part of application No. 10/325,839”) [App. 17]. Because of this relationship, the two patents share a largely common specification. They both are directed to the abstract idea of determining whether an inmate has had unauthorized communications. The ’359 patent focuses on determining whether the inmate has had unauthorized communications because the communications are associated with a security-threat group, while the ’171 patent is directed to determining whether the inmate’s communications indicate that the inmate and an employee are fraternizing.

A. The ’359 and ’171 patents both describe a general process for determining whether an inmate has had unauthorized communications.

Fundamentally, the ’359 and ’171 patents recognize that determination of whether an inmate has had unauthorized communications can be determined through monitoring those communications. The patents explain that “[i]nmate call control systems may also include certain call monitoring facilities that enable correctional facility personnel to monitor and record inmate calls.” Appendix, Ex. A, at 1:56–59 [App. 9], Ex. B, at 1:59–62 [App. 25]. The patents recognize, however, that the correctional facilities have “limited resources for monitoring calls.” Appendix, Ex. A, at 2:1–2 [App. 9], Ex. B, at 2:4 –6 [App. 25]. The patents admit that it was well-known for correctional facilities to maintain call detail records of inmate calls, typically

including "the name of the inmate (and/or inmate identification number), the inmate's location, the number called and the date, time and duration of the call." Appendix, Ex. A, at 1:53–56 [App. 9], Ex. B, at 1:56–59 [App. 25].

To optimize the use of monitoring resources, the patents describe a method for comparing information about the calls (such as phone numbers) to stored information (such as lists of phone numbers) relating to members of security-threat groups, like gangs or terrorist organizations, or prison employees. Figure 6 in each patent shows the basic implementation for telephone communications:

'359 Patent — Security-Threat Detection

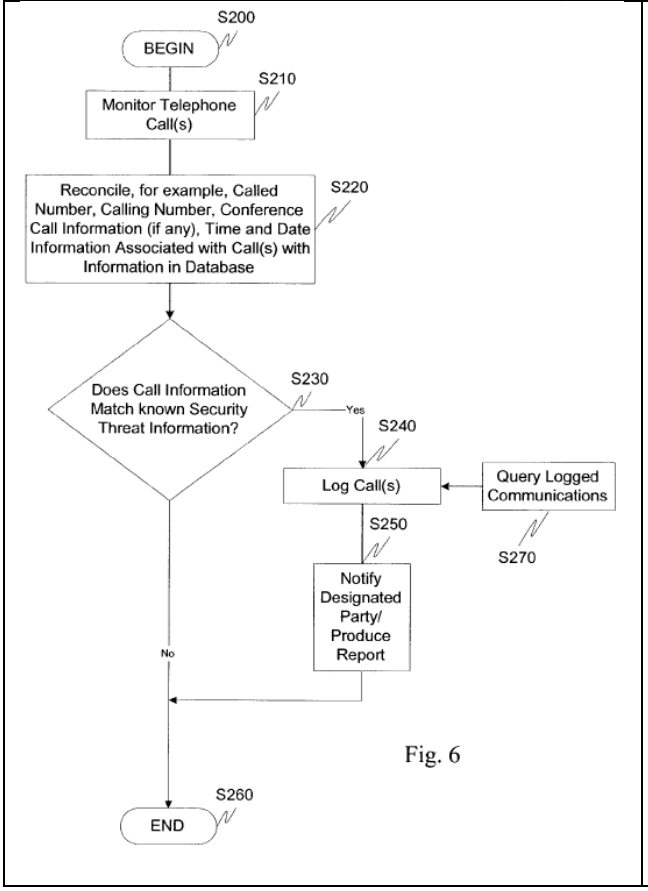

Fig. 6

[App. 8].

'171 Patent — Fraternization Detection

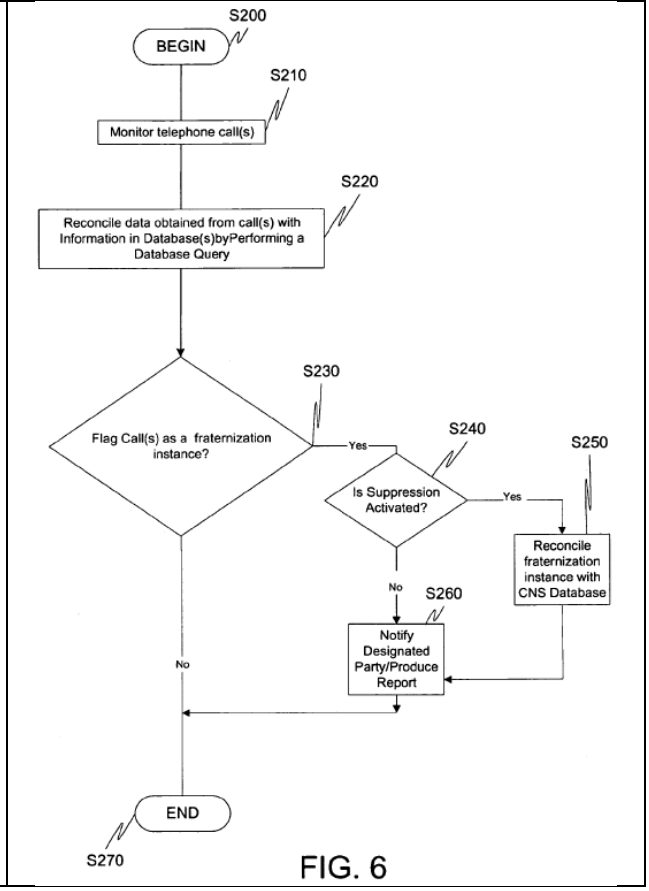

FIG. 6

[App. 24].

As shown in these figures, the basic approach is to monitor telephone calls and reconcile data from the call (e.g., called number, calling number, conference call information, time and

date) with information in a database. If the call information matches information in the database indicating either a known security threat (’359 patent) or a fraternization instance (’171 patent) the call information is further analyzed. In the ’359 patent, if a threat-group contact is detected, the call is logged, and a designated party is notified of the unauthorized communication and/or a report is produced. *See* Appendix, Ex. A, at 10:45 to 11:3 [App. 13–14].

The procedure is the same for the ’171 patent with one minor difference. Unlike communications with known security-threat-group members, in some instances, inmates are permitted to communicate with certain employees without it being indicative of fraternization. One example described by the ’171 patent is where the inmate has a relative who is a corrections officer. *See* Appendix, Ex. B. at 4:63 to 5:6 [App. 26–27]. Because the inmate’s communications with his relative should not be considered improper fraternization, the ’171 patent includes an additional database, a “called number suppression (CNS)” database, that contains “safe harbor” employee contact points. *Id.* at 4:54–57 [App. 26].

Referring again to Figure 6 of the ’171 patent above, after a call is flagged as potential fraternization, it is next determined whether to analyze the call information further to check if the call information falls within the “safe harbor” of the CNS database. *Id.* at 8:66 to 9:14 [App. 28–29]. The ’171 patent shows that this supplemental check is optional. *Id.* If the call number suppression is not applied, just like in the ’359 patent, a designated party is notified of the potential fraternization and/or a report is generated. *Id.* at FIG. 6. [App. 24]. If call number suppression is applied, the exact same result is achieved — a designated party is notified of the potential fraternization and/or a report is generated — but only after the call information is further reconciled with the CNS database to determine whether the call information falls within the “safe harbor” information in the CNS database. *Id.* at 8:66 to 9:21, FIG. 6 [App. 28–29, 24].

In various places, the patents describe the "database" as being an electronic database on a database server, *see, e.g.*, Ex. A at 3:9, 4:31 [App. 10], Ex. B at 3:43, 6:23 [App. 26, 27], but fundamentally, the exact communication-analysis method can be performed using paper-record files containing the same information. For example, in the patents, each and every step in the Figure 6 flowcharts is capable of being performed by a manual comparison of the call information to threat-group information in a paper file ('359 patent) or of the call information to correction-facility employee information in a paper file ('171 patent). Likewise, the CNS database for "safe harbor" employee information could similarly be a paper file that is checked manually.

B. The '359 and '171 patents describe and claim nothing more than comparing a first piece of information to a database of information.

Fundamentally, the '359 and '171 patents are nothing more than an inmate-communications implementation of an authorization list similar to those people encounter every day. Perhaps the most obvious example of an authorization list is dining at a reservations-required restaurant. When the customer arrives, he or she is asked for a first piece of information — his or her name. The restaurant employee compares that first information to a database of stored information, namely the list of reservations. If the first information (the name) matches the second information (the reservations), then the restaurant takes an action and seats the customer. If the information doesn't match, the customer is turned away.

There are also numerous examples of where a first piece of information is compared against a database of information to ensure that security is maintained. A person attempting to enter a secured facility (including a correctional institution) must present information in the form of identification, and the facility compares that information, either electronically or manually, to

a database of stored information, namely the list of the persons authorized to access the facility. If there is a match, the facility takes action by granting the person access.

Some examples involve taking certain actions when a security risk is determined after comparing a first piece of information to a database of stored information. A police officer patrolling the streets may check license-plate numbers of suspicious vehicles (i.e., first information) against a number of databases, including lists of stolen vehicles or vehicles associated with persons having open arrest warrants (i.e., second information). If there is a match the officer may take action by stopping the motorist, arresting the person, impounding the vehicle, writing a report, etc.

The ’359 and ’171 patents are no different than these examples. They simply apply in the inmate-communication context the age-old concept of comparing a first piece of information (e.g., inmate call information) to a list or database of stored information (e.g., security-threat-group information or employee information) to see if there is a match. Applying a generic idea to a specific situation does not render it patentable, especially where, as here, the patent claims recite only generic computer components to implement the idea.

III. LEGAL STANDARDS

A. Standard for motion for judgment on the pleadings under Rule 12(c).

Rule 12(c) of the Federal Rules of Civil Procedure provides that “[a]fter the pleadings are closed — but early enough not to delay trial — a party may move for judgment on the pleadings.” *Loyalty Conversion Sys. Corp. v. Am. Airlines*, No. 2:13–CV–655, 2014 WL 4364848, at *4 (E.D. Tex. Sept. 3, 2014) (Bryson, J.) (alteration in original) (deciding subject-matter eligibility under § 101 on Rule 12(c) motion. A motion under Rule 12(c) “is designed to dispose of cases where the material facts are not in dispute and a judgment on the merits can be rendered by looking to the substance of the pleadings and any judicially noticed facts.” *Id.* The

legal standards governing a motion under Rule 12(c) are the same as those governing a motion under Rule 12(b)(6). *Johnson v. Johnson*, 385 F.3d 503, 529 (5th Cir. 2004). Thus, the ultimate question for the court in deciding a Rule 12(c) motion is whether, viewed in the light most favorable to the plaintiff, the complaint states a valid claim for relief. *Loyalty Conversion*, 2014 WL 4364848, at *4. A motion for judgment on the pleadings under Rule 12(c) should be granted if the complaint lacks a cognizable legal theory. *Jericho Sys.*, 2015 WL 2165931, at *1.

B. Patent eligibility is appropriately resolved at the pleading stage.

The question of whether a claim recites patentable subject matter under § 101 is a question of law. *See, e.g.*, *Accenture Global Servs. GmbH v. Guidewire Software, Inc.*, 728 F.3d 1336, 1340–41 (Fed. Cir. 2013); *Dealertrack, Inc. v. Huber*, 674 F.3d 1315, 1333 (Fed. Cir. 2012). Courts routinely address patent eligibility under § 101 as a threshold inquiry and resolve it as a matter of law at the pleading stage. *See, e.g.*, *Content Extraction & Transmission, LLC v. Wells Fargo Bank Nat'l Ass'n*, 776 F.3d 1343, 1349 (Fed. Cir. 2014); *Jericho*, 2015 WL 2165931, at *1.

In fact, as recently explained by Judge Mayer of the Federal Circuit, § 101 inquiries present a threshold issue: "Failure to recite statutory subject matter is the sort of 'basic deficiency,' that can, and should, 'be exposed at the point of minimum expenditure of time and money by the parties and the court.'" *OIP Techs., Inc. v. Amazon.com, Inc.*, 788 F.3d 1359, 1364 (Fed. Cir. 2015) (Mayer, J., concurring) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 558 (2007)). Where, as here, asserted claims are plainly directed to a patent-ineligible concept, the Federal Circuit has "repeatedly sanctioned a district court's decision to dispose of them on the pleadings." *Id.* at 1365.

C. The Court may consider the pleadings, documents attached to or referenced in the pleadings, and material subject to judicial notice.

In deciding this motion, it is appropriate for the Court to consider both GTL's Third Amended Counterclaims and the asserted patents, which are referenced in the Third Amended Counterclaims and are central to GTL's patent-infringement claims. *See, e.g.*, *Genetic Techs. Ltd. v. Bristol-Myers Squibb Co.*, No. 12–394–LPS, No. 12–396–LPS, 2014 WL 5507637, at *3 (D. Del. Oct. 30, 2014); *Gorski v. The Gymboree Corp.*, No. 14–CV–01314–LHK, 2014 WL 3533324, at *2 (N.D. Cal. July 16, 2014) (holding that "the Court may consider on a Rule 12(b)(6) motion not only documents attached to the Complaint, but also documents whose contents are alleged in the complaint"); *see also Morlock, L.L.C. v. JP Morgan Chase Bank, N.A.*, 587 F. App'x 86, 87 n.3 (5th Cir. 2014) ("We note approvingly . . . that various other circuits have specifically allowed that '[d]ocuments that a defendant attaches to a motion to dismiss are considered part of the pleadings if they are referred to in the plaintiff's complaint and are central to her claim.'") (quoting *Collins v. Morgan Stanley Dean Witter*, 224 F.3d 496, 498–99 (5th Cir. 2000)) (alteration in original). The Court may also take judicial notice of and consider the prosecution history of the asserted patents in the PTO because prosecution histories are public records whose accuracy cannot reasonably be questioned. *See Genetic Techs.*, 2014 WL 5507637, at *3 (citing *Hockerson-Halberstadt, Inc. v. Avia Group Int'l, Inc.*, 222 F.3d 951, 957 (Fed. Cir. 2000)); *Iconfind, Inc. v. Google, Inc.*, No. 2:11–CV–0319–GEB–JFM, 2012 WL 158366, at *1 (E.D. Cal. Jan. 18, 2012) (quoting Fed. R. Evid. 201) (taking judicial notice of the asserted patent's prosecution history because it is "a public record that is 'capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned'"); *see also Morlock*, 587 F. App'x at 87 n.3 ("[I]t is clearly proper in deciding a 12(b)(6) motion to take judicial notice of matters of public record.").

D. Standard for patentable subject matter under 35 U.S.C. § 101.

The Patent Act states "[w]hoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title." 35 U.S.C. § 101. But this provision contains an important implicit exception — laws of nature, natural phenomenon, and abstract ideas are not patentable.

In *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*, the Supreme Court set forth a framework for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts. *Mayo*, 132 S. Ct. at 1297–98. The Court recently reaffirmed that two-step test for determining subject-matter eligibility under § 101 in *Alice Corp. Pty. Ltd. v. CLS Bank International*, 134 S. Ct. 2347, 2355–57 (2014). Under the test, an alleged invention falls outside § 101 and is unpatentable if (1) "the claims at issue are directed to a patent-ineligible concept," i.e., a law of nature, natural phenomenon, or abstract idea, and (2) the "additional elements" set forth in the claims do not supply an "inventive concept" (i.e., transform the nature of the claim into a "new and useful application" of the ineligible concept in the physical realm) that ensures that the patent covers something "significantly more than" the ineligible concept itself. *Id.* at 2355 (citing *Mayo*, 132 S. Ct. at 1297–98); *Jericho Sys.*, 2015 WL 2165931, at *2.

The first step of the *Mayo* test requires a court to determine whether the claims at issue are directed to one of the three patent-ineligible concepts, i.e., a law of nature, natural phenomenon, or abstract idea. *Mayo*, 132 S. Ct. at 1293–94, 1297. Although the Supreme Court has not provided a definition of an "abstract idea," it has provided examples through its opinions: mitigating risk, organizing human activities, and creating contractual relationships. *See Alice*, 134 S. Ct. at 2355–57; *Bilski v. Kappos*, 561 U.S. 593, 611 (2010); *see also Content Extraction*,

776 F.3d at 1347 ("The Supreme Court has not 'delimit[ed] the precise contours of the "abstract ideas" category.'") (quoting *Alice*, 134 S. Ct. at 2357).

The second step requires "a search for an inventive concept" beyond the law of nature or abstract idea itself. *Mayo*, 132 S. Ct. at 1294, 1298. In other words, if the answer to the question in the first step is yes (i.e., the claims at issue are directed to a patent-ineligible concept), then the Court next considers the elements of each claim both individually and "as an ordered combination" to determine whether additional elements "transform the nature of the claim" into a patent-eligible application. *Id.* An "inventive concept" is an element or combination of elements that is "sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself." *Id.* at 1294.

In this second *Mayo* step, what is *not* sufficient is the mere addition of "well-understood, routine, conventional activit[ies]," such as "conventional computer activities or routine data-gathering steps." *OIP Techs.*, 788 F.3d at 1363 (alteration in original) (quoting *Alice*, 134 S. Ct. at 2359). Neither implementation of an abstract idea using generic computer components, nor limitation to a particular technological field, constitutes an inventive concept beyond the ineligible subject matter itself. *See Alice*, 134 S. Ct. at 2358; *buySAFE, Inc. v. Google, Inc.*, 765 F.3d 1350, 1355 (Fed. Cir. 2014) (collecting cases); *Accenture*, 728 F.3d at 1345; *see also Loyalty Conversion*, 2014 WL 4364848, at *10. "Given the ubiquity of computers, wholly generic computer implementation is not generally the sort of 'additional featur[e]' that provides any 'practical assurance that the process is more than a drafting effort designed to monopolize the [abstract idea] itself.'" *Alice*, 134 S. Ct. at 2358 (alteration in original) (citations omitted) (quoting *Mayo*, 132 S. Ct. at 1297).

IV. POINTS AND AUTHORITIES

According to the two-part *Mayo* test, the '359 and '171 patents are ineligible for patent protection under § 101 because (1) their claims are directed to a patent-ineligible abstract idea — determining if an inmate has had unauthorized communications — and (2) the additional, generic computer and data-gathering limitations do not supply an inventive concept sufficient to transform the claims into patent-eligible application of that abstract idea.

A. The claims of the '359 and '171 patents are directed to the ineligible abstract idea of determining if an inmate has had unauthorized communications.

As explained above, the first step of the *Mayo* analysis requires determining whether a claim is "directed to" subject matter in one of the three excluded categories: laws of nature, natural phenomena, and abstract ideas. Here, the claims of the patents describe methods and systems for comparing information about inmate communications (e.g., telephone numbers) to stored information (e.g., telephone numbers) about correctional-facility employees or that is associated with security threat groups to determine if the inmate is having unauthorized communications. If improper communications are identified, the patents describe taking some action, such as generating a report.

The patents acknowledge that collecting and storing the type of information in this comparison was known before the application. Specifically, the patents acknowledge in the "Background" section:

> Correctional facilities maintain control systems for processing inmate calls. Each time an inmate places a call from a correctional facility, a call detail record (CDR) of the call is created. The call detail records of inmate calls typically include the name of the inmate (and/or inmate identification number), the inmate's location, the number called and the date, time and duration of the call.

Appendix, Ex. A, at 1:50–56 [App. 9], Ex. B, at 1:53–59 [App. 25]. Likewise, the ’359 patent describes additional existing databases containing information about security-threat groups and inmates. Specifically, the patent discusses the Department Offender Tracking System (DOTS) database, which the patent explains is “a database of known gang information and affiliations” that is maintained by the Department of Corrections and provides information about security-threat groups and inmates known to be affiliated with security-threat groups. Appendix, Ex. A at 3:66 to 4:7 [App. 10]. Also disclosed is the TIES database, which “includes information about all of the inmates of a DOC facility, including information such as inmate Personal Identification Numbers (PIN), housing unit, lock, and the like.” *Id.* at 4:7–10 [App. 10]. And while the ’171 patent is not explicit about using a pre-existing database of employee information for the fraternization database, obviously it was well known for employers to maintain databases of information about their employees that include contact information such as telephone numbers.

1. The ’359 patent claims fail the first step of the Mayo analysis.

GTL has asserted three independent claims in the ’359 patent against Securus, namely claims 1, 13, and 14. Appendix, Ex. C at 1 (listing asserted claims) [App. 32]. As shown by the comparison chart below, all of the claims are related to determining whether an inmate’s communications are prohibited because they are associated with a security-threat group :

1. A method for identifying telephone call activities that pose potential security threats, comprising: storing first information regarding security threat groups; storing second information regarding inmates known to be affiliated with the security threat groups; storing call detail records associated with telephone calls to or from inmates associated with a correctional facility; and using the call detail records and the first and second information to identify telephone call activity associated with one of the security threat groups.	13. A computer-readable medium that stores instructions executable by at least one processor, comprising: instructions for storing first information regarding security threat groups; instructions for storing second information regarding inmates known to be affiliated with the security threat groups; instructions for storing communication detail records associated with electronic communications to or from inmates associated with a correctional facility; and instructions for analyzing the communication detail records against the first and second information to identify electronic communication activity associated with one of the security threat groups.	14. A system, comprising: a memory to store: information regarding security threat groups and inmates known to be affiliated with the security threat groups, and communication detail records associated with communications to or from inmates associated with a plurality of correctional facilities; and an analysis module to analyze the communication detail records against the information regarding security threat groups and inmates known to be affiliated with the security threat groups to identify communication activity associated with one of the security threat groups.
[App. 14].	[App. 15].	[App. 15].

The asserted dependent claims of the ’359 patent (claims 2–8, 11, 15–17, 20 and 21) simply provide specific examples of the type of information used in the broader claims. Claims 2 and 15 specify that the “information regarding security threat groups” includes “information regarding at least one of inmate organizations, inmate groups, inmate alliances, or gangs.” Claims 3 and 4 require, respectively, storing of call records and establishing correlations of inmate calls, from a plurality of correctional facilities. Claim 5 also requires storing of “information regarding each inmate associated with the correctional facility” and using that data in the security-threat-group analysis. Claim 6 further requires “regularly updating the first and second information” that is stored, while claim 7 requires “automatically recording a name of an inmate who calls a telephone number” associated with one of the security-threat groups. Claims

8, 17 and 20 require identification and tagging of communications possibly related to security-threat groups. Claim 11 is directed to tagging calls by two or more inmates to the same external number as possibly related to a security-threat group. Claim 16 requires correlation of communications to "identify communication activities associated with the security threat groups." Finally, claim 21 provides that the communications for which records are stored and analyzed "include at least one of telephone calls, electronic mail transmissions, or instant message transmissions." Appendix, Ex. A at cols. 12–14 [App. 14–15].

While the claims contain slight variations, all of them are directed to determining if an inmate has had unauthorized communications because they indicate potential association with a security-threat group. Fundamental processes like this, however, are explicitly ineligible for patent protection under the Supreme Court's directives in cases like *Bilski*, *Mayo,* and *Alice* because "monopolization of those tools through the grant of a patent might tend to impede innovation more than it would tend to promote it." *Mayo,* 132 S. Ct. at 1293. This case is no different.

2. The '171 patent claims fail the first step of the Mayo analysis.

GTL has asserted four independent claims in the '171 patent against Securus, namely claims 1, 9, 17 and 23. Appendix, Ex. C at 1 (listing asserted claims) [App. 32]. As shown by the comparison chart below, all of the claims are related to determining whether an inmate's communications are unauthorized because they indicate fraternization between the inmate and an employee of the correctional facility:

1. A method of discovering inmate-employee fraternization comprising: monitoring a plurality of inmate communications; comparing the plurality of monitored inmate communications to information relating to inmates and employees located in a database; determining, based at least on the results of the comparing, if one or more of the plurality of communications indicate that an employee and inmate are fraternizing; and performing a predetermined action if one of the plurality of communications indicates that the employee and inmate are fraternizing.	9. A system that discovers employee-inmate fraternization comprising: a monitoring module that monitors a plurality of communications from inmates; a comparison module that compares the plurality of monitored communications to information relating to inmates and employees in a database; a determination module that determines, based at least on the results of the comparison, if one or more of the plurality of communications indicate that an employee and an inmate are fraternizing; and a result module that forwards instructions to perform a predetermined action if one of the plurality of communications indicates that the employee and the inmate are fraternizing.
[App. 29].	[App. 29].

17. An information storage media comprising information configured to discover inmate-employee fraternization comprising: information that monitors a plurality of communications from inmates; information that compares the plurality of monitored communications to information relating to inmates and employees in a database; information that determines, based at least on the results of the comparing, if one or more of the plurality of communications indicates that an inmate and an employee are fraternizing; and information that performs a predetermined action if one of the plurality of communications indicates that an inmate and an employee are fraternizing.	23. A method of discovering inmate-employee fraternization comprising: receiving a communication from an inmate; comparing the communication to information relating to inmates and employees located in a database; determining, based at least on the results of the comparing, whether the communication indicates that an employee and inmate are fraternizing; and performing a predetermined action if the communication indicates that the employee and inmate are fraternizing.
[App. 30].	[App. 30].

The asserted dependent claims of the ’171 patent (claims 2, 5–8, 10, 13–16, 27) simply provide specific examples of the type of information or actions in the broader claims. Claim 2 specifies that the “predetermined action is at least one of generating a report or sending a

notification to at least one entity." Claims 5, 13, and 27 provide that the communications are electronic messages, instant messages, or telephone calls. Claims 6 and 14 specify that the communications "can be monitored at least one of locally, nationally or internationally." Claims 7 and 15 detail that the information collected is "at least one of a called number, time and date information, sender information, recipient information, location information, called identification information or inmate identification." Finally, claims 8 and 16 provide for querying "a database of logged monitored communications to determine potential fraternization between an employee and an inmate." Appendix, Ex. B at cols. 10–12 [App. 29–30].

As in the '359 patent, the asserted claims in the '171 patent contain slight variations, but all of '171 patent claims are directed to determining if communications are prohibited because they are indicative of potential fraternization between employees and inmates. Importantly, for purposes of this motion, there are no meaningful distinctions between the system and method claims of either the '359 or '171 patents, as all the claims recite the same fundamental abstract idea. Although system claims are formally drawn to eligible subject matter (in § 101 terms, a "machine"), the system claims here are no different from the method claims in substance. Like the claims at issue in *Alice*, the method claims here are directed to an ineligible concept implemented using a generic computer, and the system claims recite a handful of generic components (e.g., microprocessor, memory) configured to implement the same idea. *See Alice*, 134 S. Ct. at 2358–60. Thus, lest "the determination of patent eligibility 'depend simply on the draftsman's art,'" both sets of claims are analyzed using the same *Mayo* framework, and rise or fall together. *Id.* at 2358–60; *see Accenture*, 728 F.3d at 1344 (holding when system and method claims "contain only 'minor differences in terminology [but] require performance of the same basic process,' they should rise or fall together") (alteration in original) (citations omitted);

Bancorp Servs., L.L.C. v. Sun Life Assur. Co. of Can. (U.S.), 687 F.3d 1266, 1277 (Fed. Cir. 2012) (holding that "[t]he district court correctly treated the system and method claims at issue in this case as equivalent for purposes of patent eligibility under § 101").

B. The additional elements — generic computers, databases, software, and storage, all performing conventional tasks — do not supply an inventive concept.

Because the claims of the '359 and '171 patents are directed to a patent-ineligible abstract idea, the analysis turns to the second step of *Mayo*'s framework, which examines the additional elements of the claims to determine whether they contain an inventive concept that ensures the patent covers something "significantly more than" the patent-ineligible matter itself. *Mayo*, 132 S. Ct. at 1293–94; *see also Alice*, 134 S. Ct. at 2357; *buySAFE*, 765 F.3d at 1353. The inventive concept must be sufficient to "transform" the claimed abstract idea into a patent-eligible application. *Alice* and *Mayo* make clear that to transform an unpatentable abstract idea into a patent-eligible *application* of such an idea, a patent must do more than simply state the abstract idea while adding the words "apply it." *See Alice*, 134 S. Ct. at 2357; *Mayo*, 132 S. Ct. at 1294. And the prohibition against patenting ineligible concepts cannot be circumvented by attempting to limit the use of the concept to a particular technological environment. *See Bilski*, 130 S. Ct. at 3230.

To begin with, to the extent the '359 and '171 patents add anything to the abstract idea of determining whether an inmate's communications are unauthorized, the patents add only basic electronic implementation accomplished by a general-purpose computer and conventional computer components. *See, e.g.*, '359 patent, claim 13 ("computer-readable medium," "processor"), claim 14 ("memory"); '171 patent, claim 17 ("information storage media"). Indeed, as discussed above, the only element in claim 1 of the '359 patent that even remotely suggests a computerized process is "storing," even though it is beyond question that information can be stored in paper

records and files. Similarly, claim 1 of the '171 patent requires a "database," which could be a paper file, but even if limited to a computerized database, is entirely generic.

The patent specifications are telling in this regard. Both patents are explicit that the alleged inventions can be implemented in hardware or software or on any type of general computer equipment. Likewise, the claims merely incorporate a variety of *purely conventional* elements that are *entirely generic*. The specifications state:

- **Any generic computer:** "As illustrated in the figures, the present invention can be implemented either on a single programmed ***general purpose computer***, a separate programmed ***general propose computer***, or a combination thereof. However, the present invention can also be implemented on a special purpose computer, a programmed microprocessor or microcontroller and peripheral integrated circuit element, an ASIC, or other integrated circuit, a digital signal processor, a hard-wired electronic or logic circuit, such as discrete element circuit, a programmable logic device, such as a PLD, PLA, FPGA, PAL or the like. In general, ***any device*** capable of implementing a state machine that is in turn capable of implementing the flowcharts illustrated herein can be used to implement the present invention." Appendix, Ex. B, at 9:24–38 (emphasis added) [App. 29]; *see also* Ex. A, at 11:4–20 [App. 14].

- **Software or hardware or both:** "Furthermore, the disclosed method ***may be readily implemented in software*** using an object or object-oriented software development environment that provides source code that can be used on a variety of computer, server, or workstation hardware platforms. ***Alternatively, the present invention may be implemented partially or fully in hardware*** using standard logic circuits or VLSI design. Whether software or hardware is used to implement the systems in accordance with this invention is dependent on the speed and/or efficiency requirements of the system, the particular function, and the particular software or hardware systems or microprocessor or microcomputer and telecommunications systems being utilized. The present invention however, ***can be readily implemented*** in hardware and/or software ***using any know[n] or later developed systems or structures, devices and/or software by those of ordinary skill in the applicable art from the functional description provided herein, and with a general basic knowledge of the computer and telecommunications arts***." Appendix, Ex. B at 9:39–57 (emphasis added) [App. 29].; *see also* Ex. A at 11:21–40 [App. 14].

- **Generic software on a generic computer:** "Moreover, the disclosed methods ***may be readily implemented as software executed on a programmed general purpose computer***, a special purpose computer, a microprocessor, or the like. In these instances, the methods and systems of this invention ***can be***

> ***implemented as a program embedded in a telecommunications system, such as JAVA® or CGI script***, as a resource residing on a server or graphics workstation, as a routine embedded on a dedicated fraternization discovery system, or the like. ***The present invention can also be implemented by physically incorporating the system into a software and/or hardware system*** such as the hardware and software system of a server and associated interface device." Appendix, Ex. B at 9:58 to 10:3 (emphasis added) [App. 29]; *see also* Ex. A at 11:41–51 [App. 14].

The patents' explanation that the alleged inventions can be implemented any way desired — whether in software or hardware, on a single general-purpose computer, on a separate general-purpose computer, or other type of computer — underscores that certain claims' recitation of generic elements like "memory," "processor," and "information storage medium" are insufficient to transform the abstract idea into a patent-eligible application of the idea. *See OIP Techs.*, 788 F.3d at 1363 ("Both the prosecution history and the specification emphasize that the key distinguishing feature of the claims is the ability to automate or other wise make more efficient traditional price-optimization methods. . . . But relying on a computer to perform routine tasks more quickly or more accurately is insufficient to render a claim patent eligible."); *Bancorp*, 687 F.3d at 1278 (holding that a computer "employed only for its most basic function . . . does not impose meaningful limits on the scope of those claims"); *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1372–73 (Fed. Cir. 2011); *Loyalty Conversion*, 2014 WL 4364848, at *10.

V. CONCLUSION

The asserted '359 and '171 patents fall squarely within the Supreme Court's definition of patent-ineligible subject matter because their claims are directed to an abstract idea but do not include any additional inventive concept sufficient to transform the claims into a patent-eligible application of that ineligible concept. Accordingly, the patents are invalid, and GTL cannot maintain a legally cognizable claim for patent infringement. Securus therefore respectfully

moves for judgment on the pleadings, based on the invalidity of the ’359 and ’171 patents under 35 U.S.C. § 101, and requests that the Court dismiss GTL’s Third Amended Counterclaims.

Respectfully submitted,

/s/ Richard A. Sayles
Richard A. Sayles
(Lead Counsel)
Texas State Bar No. 17697500
dsayles@swtriallaw.com
Mark D. Strachan
Texas State Bar No. 19351500
mstrachan@swtriallaw.com
E. Sawyer Neely
Texas State Bar No. 24041574
sneely@swtriallaw.com
Darren P. Nicholson
Texas State Bar No. 24032789
dnicholson@swtriallaw.com

SAYLES | WERBNER, P.C.
1201 Elm Street, Suite 400
Dallas, Texas 75270
214.939.8700 – Telephone
214.939.8787 – Facsimile

Bruce S. Sostek
Texas State Bar No. 18855700
bruce.sostek@tklaw.com
Richard L. Wynne, Jr.
Texas State Bar No. 24003214
richard.wynne@tklaw.com

THOMPSON & KNIGHT LLP
One Arts Plaza
1722 Routh Street, Suite 1500
Dallas, Texas 75201
214.969.1700 – Telephone
214.969.1751 – Facsimile

G. Michael Gruber
Texas Bar No. 08555400
mgruber@ghetrial.com
Anthony J. Magee
Texas Bar No. 00786081
amagee@ghetrial.com
Robert E. Weitzel
Texas Bar No. 24070823
rweitzel@ghetrial.com

GRUBER HURST ELROD JOHANSEN
HAIL SHANK LLP
Fountain Place
1445 Ross Avenue, Suite 2500
Dallas, Texas 75202
214.855.6800 – Telephone
214.855.6808 – Facsimile

ATTORNEYS FOR PLAINTIFF/COUNTERCLAIM-
DEFENDANT SECURUS TECHNOLOGIES, INC.

CERTIFICATE OF SERVICE

I certify that on July 31, 2015, I caused a true and correct copy of the foregoing to be served via ECF on all counsel of record.

/s/ Richard A. Sayles
Richard A. Sayles